第5節 サイバー空間をめぐる動向

1 サイバー空間と安全保障

近年の情報通信技術（ICT（Information and Communications Technology））の発展により、インターネットなどの情報通信ネットワークは人々の生活のあらゆる側面において必要不可欠なものになっている。一方、重要インフラの情報通信ネットワークに対するサイバー攻撃[1]は、人々の生活に深刻な影響をもたらしうるものである。

サイバー攻撃の種類としては、情報通信ネットワークへの不正アクセスやメール送信などを通じたウィルスの送り込みによる機能妨害や情報の改ざん・窃取、大量のデータの同時送信による情報通信ネットワークの機能阻害などのほか、電力システムなどの重要インフラへのシステムダウンや乗っ取りを目的とした攻撃などがあげられる。また、インターネット関連技術は日進月歩であり、サイバー攻撃[2]も日に日に高度化、巧妙化している。

軍隊にとって情報通信は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、ICTの発展によって情報通信ネットワークへの軍隊の依存度が一層増大している。また、軍隊は任務遂行上、電力をはじめとする様々な重要インフラに依存しており、これらの重要インフラに対するサイバー攻撃が、任務の大きな阻害要因になり得る。そのため、サイバー攻撃は敵の軍隊の弱点につけこんで、敵の強みを低減できる非対称的な戦略として位置づけられつつあり、多くの外国軍隊がサイバー空間における攻撃能力を開発しているとされている。特に、中国及びロシアは、ネットワーク化された部隊の妨害やインフラの破壊などのために、軍のサイバー攻撃能力を強化していると指摘されている[3]。

また、国家などに害を加えようと意図する主体（非国家主体を含む）は、物理的な手法による直接攻撃よりも、サイバー空間を通じた攻撃を選択する方がより容易である場合が多いと認識している可能性が高い[4]。さらに、情報収集目的のために他国の情報通信ネットワークへの侵入が行われているとの指摘があり、より多くの機微な情報がサイバー空間に保管されるようになるにつれ、こうしたサイバー攻撃による情報窃取の被害はより重大なものとなってきている。

2 サイバー空間における脅威の動向

このような状況のもと、諸外国の政府機関や軍隊などの情報通信ネットワークに対するサイバー攻撃が多発している[5]。

これらの一部については、中国の人民解放軍[6]、

1 サイバー攻撃の標的には、大きくは国家間などの地球規模のほか、国や政府機関、地域社会、経済界やインフラ、企業、個人まで様々なものがある。そのためサイバー攻撃への対策は、それぞれの規模に対して最適な対策が必要であると言われている。
2 12（平成24）年9月、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」では、サイバー攻撃の特徴として①多様性：実行者、手法、目的、状況などが多様であること、②匿名性：実行者の隠蔽（いんぺい）・偽装が容易であること、③隠密性：攻撃の存在を察知し難いものや、被害発生の認識すら困難であること、④攻撃側の優位性：手法によっては攻撃手段の入手が容易であることや、ソフトウェアのぜい弱性を完全に排除することが困難であること、⑤抑止の困難性：報復攻撃や防御側の対策による抑止効果が小さいことなどがあげられている。
3 米国防情報局長官世界脅威評価（18（平成30）年3月）による。
4 16（平成28）年2月、オバマ米大統領（当時）が発表した「サイバーセキュリティ国家行動計画」による。
5 米行政予算管理局が連邦情報セキュリティ管理法に基づき議会に報告している年次報告書によると、17米会計年度に連邦政府機関から報告されたサイバーセキュリティ・インシデントの件数は、35,277件。また、18（平成30）年2月の米国家情報長官「世界脅威評価」は、米国に対して最も重大なサイバー脅威を与える主体として、ロシア、中国、イラン及び北朝鮮を挙げ、それぞれ、①ロシアは米国及びその同盟国の重要インフラの偵察を継続するとともに、米国の政策への洞察を得るため、米国、NATO及びその同盟国を標的とする、②中国は引き続き、国家安全保障上の優先事項を支えるため、サイバー諜報を実施するとともにサイバー攻撃能力を向上させる、③イランは、諜報及び将来的なサイバー攻撃の準備のため、米国及びその西側同盟国への浸透活動を継続する、④北朝鮮は、資金獲得、情報収集並びに韓国及び米国に対する攻撃を実施するためにサイバー活動を利用する、との見解を示している。ISILによるサイバー空間の利用については、Ⅰ部3章1節を参照
6 13（平成25）年2月の米国情報セキュリティ企業「マンディアント」の「APT1：中国のサイバー諜報部隊の1つを暴露する」は、米国などに対する最も活動的なサイバー攻撃集団は、中国人民解放軍総参謀部第3部（当時）隷下の「61398部隊」であると結論づけている。またサイバー部隊である総参謀部第3部（当時）は、13万人の規模であるとの指摘がある。

情報機関、治安機関、民間ハッカー集団や企業など様々な組織の関与が指摘[7]されている。15（平成27）年5月に発表された中国の国防白書「中国の軍事戦略」[8]によれば、中国はサイバー戦力の建設を加速させるとしているほか、同年12月末、中国における軍改革[9]の一環として創設された「戦略支援部隊」のもとにサイバー戦部隊が編成されたとの指摘もある。15（平成27）年6月には、米国連邦人事管理局がサイバー攻撃を受け、米連邦職員や米軍軍人などのおよそ2,200万人分の個人情報が窃取されていたことが判明し、中国の関与が指摘[10]されたが、中国は政府の関与を否定し、ハッカーによる「犯罪」だと説明している。また、17（平成29）年4月には、中国の政府機関と関連がある2つのハッカーグループが韓国の政府、軍、防衛企業などに対してサイバー攻撃を行ったとの指摘[11]がある。中国はサイバー攻撃により、他国の軍の作戦計画や国家安全保障の意思決定のプロセス、重要インフラなどに関する機微な情報を得ているとの指摘[12]がなされている。

15（平成27）年12月、ウクライナで大規模な停電を発生させたサイバー攻撃[13]は、ロシアの関与が指摘されており、17（平成29）年6月に、ウクライナを中心に各国で発生したランサムウェアによるサイバー攻撃については、米英両政府は18（平成30）年2月、ロシア軍によるものと発表した。また、米国政府は、ロシア情報機関が16（平成28）年の米大統領選挙の影響工作のためサイバー攻撃を行ったと批判した[14]ほか、17（平成29）年3月には、米大手インターネット企業から5億件以上の個人情報が流出したサイバー攻撃を実施したとして、ロシア連邦保安庁（FSB: Federal Security Service）の要員2名を含む4名のハッカーを起訴した[15]。ロシアについては、軍や情報機関、治安機関などがサイバー攻撃に関与しているとされる。また、軍による独自のサイバー部隊[16]の存在が明らかとなっており、敵の指揮・統制システムへのマルウェア（破壊工作プログラム）の挿入を含む攻撃的なサイバー活動を担うと指摘されている[17]。こうしたロシアによる活動の背景には、ロシアの意思決定を支援するための情報収集、軍事・政治的目的を支援するための工作、将来の有事に備えたサイバー空間の環境整備の継続などの目標があると指摘されている[18]。

16（平成28）年9月に発生した韓国軍内部ネットワークへのサイバー攻撃について、17（平成29）年5月に、韓国国防部は北朝鮮ハッカー組織と推定される勢力によるものとの結論を下したと報じられた[19]。また、このサイバー攻撃による軍事機密文書の流出が指摘されている。さらに、17（平成29）年5月には、マルウェア「ワナクライ」により、世界150か国以上の病院、学校、産業な

7 米中経済安全保障再検討委員会の年次報告書（16（平成28）年11月）は、中国は国家安全部と軍の組織によるサイバー諜報に加え、中国の多数の非国家主体が米国を標的としたサイバー諜報を実施しており、こうした主体には、政府と契約したハッカー、民間の「愛国ハッカー」、犯罪組織が含まれていると指摘している。
8 同国防白書では、「サイバー空間は、経済・社会発展の新たな支柱であり、国の安全保障の新分野である」、「サイバー空間における国際間の戦略競争は日増しに激化しており、多くの国がサイバー空間における軍事力を発展させている」、さらに、「中国はハッカー攻撃の最大の被害国の一つである」などと指摘している。
9 15（平成27）年9月以降、中国は軍改革に関する一連の決定を公表しており、16（平成28）年1月には戦略支援部隊などの新設が発表された。同部隊の任務や組織の細部は公表されていないものの、宇宙・サイバー・電子戦を担当しているとの指摘がある。
10 米中経済安全保障再検討委員会の年次報告書（15（平成27）年11月）による。この他にも、米国連邦人事管理局（OPM：Office of Personnel Management）と同じ手口で、米国の航空会社への攻撃が行われたとしている。
11 17（平成29）年7月、米中経済安全保障再検討委員会による報告書による。
12 17（平成29）年11月、米中経済安全保障再検討委員会による年次報告書による。
13 16（平成28）年2月の米ニューヨークタイムズ紙は、クリミア併合などで対立するロシア軍関与の疑いがあると報じた。
14 16（平成28）年10月の米国土安全保障省と米国家情報長官による共同声明、また、同年12月、ロシアによる米国へのサイバー攻撃に関する米国土安全保障省及びFBIの共同報告書及び、17（平成29）年1月の米大統領選に対するロシアのサイバー攻撃に関する米情報コミュニティの報告書による。なお、17年（平成29）年のフランス大統領選挙期間中には、ロシアに対して強硬姿勢と評されるマクロン氏が、サイバー攻撃に加えて、租税回避地に隠し財産があるかのようなフェイクニュースを拡散される被害に遭ったとされる。同氏は大統領就任後、仏露大統領共同記者会見の場において、ロシアメディアを虚偽宣伝団体だと名指しで非難した。
15 14（平成26）年に発生。このほか、このインターネット企業からは、13（平成25）年にもサイバー攻撃を受けて30億人分の情報が流出している。
16 17（平成29）年2月、ロシアのショイグ国防相の下院議員の説明会での発言による。発言によれば、ロシア軍に「情報作戦部隊」が存在すると明らかにされ、欧米との情報戦が起きているとし「政治宣伝活動に対抗するため」と強調、防衛目的との認識を示した。また、ロシアのサイバー軍の要員は約1, 000人との指摘がある。
17 15（平成27）年9月、クラッパー米国家情報長官（当時）が下院情報委員会で「世界のサイバー脅威」について行った書面証言による。
18 米国家情報長官世界脅威評価（17（平成29）年5月）による。
19 17（平成29）年5月の韓国・国防日報電子版による。また、攻撃に使われたIPアドレス（インターネット上の住所）の中の一部が、既存の北朝鮮ハッカーが使用していた中国・瀋陽地域のものと識別されたと指摘されている。

どのコンピュータを暗号化し、使用不能にするサイバー攻撃が行われた。この事案について、米国は、同年12月、北朝鮮によるものであるとした[20]。このサイバー攻撃により14万ドル分のビットコインが集められたとの指摘があるほか、韓国国家情報院は北朝鮮が仮想通貨を奪うために韓国の取引所などへのハッキングを繰り返しており、数百億ウォン（数十億円）相当を奪っていると報告したとされるなど、資金獲得目的のサイバー攻撃であったとの指摘がある。北朝鮮については、このようなサイバー攻撃への政府機関などの関与[21]のほか、国家規模で人材育成を行っているとの指摘もある[22]。

なお、わが国においても、15（平成27）年5月には、日本年金機構がサイバー攻撃を受け、年金の受給者と加入者の個人情報が流出した。このほか、政府の関与が指摘されているハッカー集団からの政府機関や防衛・航空宇宙産業などに対するサイバー攻撃が指摘されている。

さらに、意図的に不正改造されたプログラムが埋め込まれた製品が企業から納入されるなどのサプライチェーンリスクや、産業制御システムへの攻撃を企図した高度なマルウェアの存在も指摘されている[23]。16（平成28）年に発生したマルウェア「Mirai」によるサイバー攻撃など、IoT機器を踏み台にした攻撃が顕著化しており、その脅威は今後も増大するものと予想されている[24]。

政府や軍隊の情報通信ネットワーク及び重要インフラに対するサイバー攻撃[25]は、国家の安全保障に重大な影響を及ぼし得るものであり、また、近年、国家が関与するサイバー攻撃が増加しているとの指摘もあることから、サイバー空間における脅威の動向を引き続き注視していく必要がある。

3 ■ サイバー攻撃に対する取組

こうしたサイバー空間における脅威の増大を受け、各国において、政府全体レベル及び国防省を含む関係省庁レベルなどで、各種の取組が進められている[26]。

近年新たな安全保障上の問題となっているサイバー攻撃に関しては、効果的な対応を可能とするうえで整理すべき論点が指摘されている。例えば、サイバー空間に関しては、国際法の適用のあり方など、基本的な点についても国際社会の意見の隔たりがあるとされ、米国や欧州、わが国などは、自由なサイバー空間の維持[27]を訴え、ロシアや中国、新興国などの多くは、サイバー空間の国家管理の強化を訴えているなど、各国の主張は対立しているとの指摘もある。こうした状況を背景に、国際社会においては、サイバー空間における法の支配の促進を目指す動きがある。国連のサイバー

20 ボサート米大統領補佐官の記者会見による。なお、JPCERT/CCによると、日本では600か所、2,000端末以上が感染したとされている。
21 13（平成25）年11月、韓国報道各社が、韓国国家情報院が国会情報委員会の国政監査で北朝鮮のサイバー戦能力などについて明らかにしたと報じるとともに、北朝鮮の金正恩第1書記が、「サイバー戦は、核、ミサイルと並ぶ万能の宝剣である」と述べたと伝えた。また、16（平成28）年2月に議会に提出した米国防省「朝鮮民主主義人民共和国の軍事及び安全保障の進展に関する年次報告」では、北朝鮮は攻撃的なサイバー作戦能力を保有しているとしている。さらに、17（平成29）年1月、韓国の「2016国防白書」は、北朝鮮はサイバー部隊を集中的に増強し、規模は約7,000人と指摘している。
22 例えば、11（平成23）年6月の韓国の脱北者団体「NK知識人連帯」主催「2011北朝鮮のサイバーテロ関連緊急セミナー」における「北朝鮮のサイバーテロ能力」と題した発表資料は、北朝鮮のサイバー関連組織について、政府機関などの関与を指摘し、サイバー戦力養成のため、全国から優秀な人材を発掘し、専門教育を行っている、としている。
23 12（平成24）年10月、米下院情報特別委員会による「中国通信機器企業華為技術及び中興通訊が米国国家安全保障に及ぼす問題」と題する調査報告書では、米国重要インフラに対するサイバー攻撃能力や企図に対する懸念や、中国主要IT企業と中央政府、共産党、人民解放軍との不透明な関係がサプライチェーンリスクを増大させることへの強い懸念といった、国家安全保障上の脅威を理由に、中国大手通信機器メーカー「華為技術」及び「中興通訊」の製品を利用しないように勧告された。フランス、オーストラリア、カナダ、インド及び台湾などでも同様の動きがみられ、英国及び韓国などでは注意を促す動きがみられる。
24 17（平成29）年7月のサイバーセキュリティ戦略本部決定「2020年及びその後を見据えたサイバーセキュリティの在り方について-サイバーセキュリティ戦略中間レビュー-」による。
25 17（平成29）年10月に米国情報セキュリティ企業「ファイアアイ」が公表した「北朝鮮の主体、米国の電力会社にスピア・フィッシング攻撃」は、17（平成29）年9月に、北朝鮮政府との関連が濃厚とされるサイバー脅威グループによって、複数の米国電力会社にスピアフィッシング・メールによるサイバー攻撃が行われたとしている。
26 一般的に政府全体レベルでは、①サイバーセキュリティ関連部門の統合や運用部門の一元化、②専任のポストの設置や研究部門の新設及び拡充などによる政策部門及び研究部門の強化、③サイバー攻撃対処における情報機関の役割の拡大、④国際協力の重視、などの傾向があると考えられる。国防省レベルにおいても、サイバー空間における軍の作戦を統括する機関を新設するなど、サイバー攻撃への取組を国防戦略の中の重要な戦略目標と位置づけるなどの対応が進められている。
27 情報の自由な流通や政府のみならず民間企業・市民社会を含むマルチステークホルダー・アプローチなどを訴えている。

問題に関する第5会期政府専門家会合における報告書の合意は得られなかったものの、サイバー空間に関する国際会議[28]などの枠組みにおいて、国際的なルール作りなどに関する議論が行われている。

参照　Ⅲ部1章2節7項（サイバー空間における対応）

1 米国

米国では、連邦政府のネットワークや重要インフラのサイバー防護に関しては、国土安全保障省が責任を有しており、同省のサイバーセキュリティ通信室（CS&C: Office of Cybersecurity and Communications）が政府機関のネットワーク防御に取り組んでいる[29]。

米国は、17（平成29）年12月に発表した国家安全保障戦略において、多くの国がサイバー能力を影響力を行使する手段と捉えており、サイバー攻撃は、現代戦の重要な特徴となっているとしつつ、米国に対してサイバー能力を使用する相手を抑止、防御し、必要であれば打ち負かすとしている。そのため、米国は、①サイバー攻撃を特定し迅速に対応する能力の改善、②米国政府の財産、重要インフラ、情報などを守るためのサイバー手段及び専門知識向上、③必要に応じて敵に対しサイバー作戦を実施できるようにするため、米国政府の権限と手続きの統合の改善などを図る戦略方針を打ち出している。米国防省は、18（平成30）年1月に国家安全保障戦略を支えるものとされる国家防衛戦略2018を発表し、サイバー防衛、抗たん性、運用全体へのサイバー能力の統合の継続に投資していく方針を示している。また、オバマ政権下の15（平成27）年4月に公表された「米国防省サイバー戦略[30]」は、国防省は、①国防省のネットワーク、システム及び情報の防護、②サイバー攻撃による深刻な結果からの米国及びその権益の防護、③軍事作戦の支援のための統合的なサイバー能力の提供、の3つをサイバー空間における主要な任務[31]とし、当該サイバー能力には、敵国軍事システムの破壊を目的としたサイバー作戦が含まれるとしている。

米軍においては、戦略軍隷下のサイバー軍が、サイバー空間における作戦を統括することを任務としており、陸海空海兵隊の各サイバー部隊並びに国防省の情報環境を運用・防衛する「サイバー防護部隊」、国家レベルの脅威から米国の防衛を支援する「サイバー国家任務部隊」及び統合軍が行う作戦をサイバー面から支援する「サイバー戦闘任務部隊」（これら三部隊は「サイバー任務部隊」[32]と総称されている。）などから構成されていた。戦略軍隷下であったサイバー軍は、18（平成30）年5月に統合軍に格上げされ、これにより、サイバー軍司令官は、他の統合軍司令官と同様、国防長官に対して直接報告を行うことが可能となった[33]。

米国は、中国によるサイバー窃取は、国家安全保障に関する情報から機微な経済情報、米国の知的財産に至るまで、幅広く米国の利益を標的とし続けていると認識している。15（平成27）年9月、オバマ米大統領（当時）と習近平中国国家主席は首脳会談において、両国が知的財産のサイバー窃

第3章　国際社会の課題

---

28 サイバー空間に関する国際会議は、11（平成23）年にヘーグ英外相（当時）が提唱して立ち上げ、一連の会議はロンドン・プロセスと称されている。100か国以上の政府、国際機関、民間セクター、NGOなどが一堂に会し、サイバー空間における諸課題に関する包括的な議論を行う、ハイレベルかつ最大規模の国際会議であり、直近では17（平成29）年11月に開催されている。

29 国土安全保障省は、18（平成30）年5月にサイバーセキュリティ戦略を発表。20（平成32）年までに200億台以上のデバイスがインターネットに接続されることが予想され、それによりリスクも高まるとしている。

30 米国防省サイバー戦略では、ロシアや中国は先進的なサイバー能力及び戦略を獲得しているとした上で、ロシアの活動は秘密裏に行われており、その意図を読み取ることが難しいとしている。また中国は、知的財産を窃取し、中国企業に利益を与えているとしている。さらに、イラン及び北朝鮮のサイバー能力は高くないものの、米国及び米国の権益に対する敵対的な意図を公然と示しているとしている。

31 米国防省はサイバー空間における任務を遂行するために、①サイバー作戦実施のための即応的な部隊及び能力の構築・維持、②国防省の情報ネットワーク及びデータの防護並びに任務上のリスクの軽減、③関係省庁・企業などとの連携を通じた重大なサイバー攻撃からの米国及びその権益の防護体制の構築、④紛争管理におけるサイバー空間における各種手段の活用、⑤同盟国及びパートナー国との緊密な協力関係の構築、という5つの戦略構想を示している。

32 15（平成27）年4月、上院軍事委員会における米サイバー軍司令官の発言などによれば、三部隊には複数のチームが所属しているとされ、現在数十チームが活動中としている。また、州兵や予備役を活用し、18（平成30）年9月までに133チーム（サイバー国家任務部隊（13チーム）、サイバー防護部隊（68チーム）、サイバー戦闘任務部隊（27チーム）、支援チーム（25チーム））、6,200人規模にするとしている。

33 米国防省は、サイバー軍の統合軍への格上げの発表に際して、サイバー空間は、陸・海・空の領域と同様に重要であり、サイバー空間での作戦能力は、軍事的成功にとって不可欠であるとし、今後、サイバー兵器、サイバー防衛、サイバー要員の規模・能力強化が課題との認識を示している。

取を行わないことで合意[34]し、17（平成29）年11月のトランプ米大統領と習近平中国国家主席による首脳会談においても15（平成27）年の合意事項を継続するとしたが、依然として中国からのサイバー諜報が続いていると指摘[35]されている。

2 NATO

11（平成23）年6月に採択されたサイバー防衛に関する北大西洋条約機構（NATO） North Atlantic Treaty Organization の新政策及び行動計画は、①サイバー攻撃に対するNATOの政治的及び運用上の対応メカニズムを明確化し、②NATOが、加盟国によるサイバー防衛構築の支援や、加盟国がサイバー攻撃を受けた場合の支援を実施することを明確にし、③パートナー国などと協力していくとの原則を定めている。また、14（平成26）年9月、NATO首脳会議において、加盟国に対するサイバー攻撃をNATOの集団防衛の対象と見なすことで合意している。

組織面では、北大西洋理事会（NAC） North Atlantic Council がNATOのサイバー防衛に関する政策と作戦の政治的監督を行っているほか、新規安全保障課題局（ESCD） Emerging Security Challenges Division がサイバー防衛に関して政策及び行動計画を策定している。また、17（平成29）年11月には、サイバー作戦センターの新設及び加盟国が有するサイバー防衛能力のNATO任務・作戦への統合に関する方針に合意した[36]。さらに、NATOは08（平成20）年以降、NATOサイバー防衛能力を高めるためのサイバー防衛演習を毎年行っている。また、NATOは、EUとの間でサイバー安保・防衛分野での連携を進展させている[37]。

また、08（平成20）年には、NATOサイバー防衛センター（CCDCOE） Cooperative Cyber Defence Centre of Excellence がNATOのサイバー防衛に関する研究や訓練などを行う機関として認可[38]され、エストニアの首都タリンに設置された。同センターは、サイバー活動と国際法の関係に関する研究などを行っており、「タリンマニュアル」[39]を作成するなどの活動を行っている。17（平成29）年2月、同マニュアルの続編となる「タリンマニュアル2.0」が公表され、国家責任法、人権法、航空法、宇宙法、海洋法といった平時に関する法規範から、「武力の行使」や武力紛争法といった有事に関する法規範に至るまで、幅広い論点について検討が行われている。

3 英国

英国は、15（平成27）年11月の「NSS・SDSR2015」において、今後5年間で約19億ポンドをサイバー防衛能力向上のために投資し、サイバー空間における脅威を特定・分析する機能を強化していくことを明らかにした。16（平成28）年11月には、新たな「サイバーセキュリティ戦略」を公表し、英国がサイバーの脅威に対し安全かつデジタルの世界において繁栄するためのビジョンを提示した。このビジョンを達成するため、サイバー脅威に対し効果的に「防護」する手段の保持、攻撃的手段の保持による「抑止」、最先端技術の「開発」が必要としている。

政府全体のサイバーセキュリティ政策に関しては、戦略的方針を提示し、組織横断的な計画の調整などを行うサイバーセキュリティ・情報保証部（OCSIA） Office of Cyber Security and Information Assurance がある。16（平成28）年10月には、国のサイバーインシデントに対応し、官民のパートナーシップを推進するため、国家サイバーセキュリティセンター（NCSC） National Cyber Security Centre が政府通信本部（GCHQ） Government Communications Headquarters の傘下機関として新しく創設された。

34 首脳会談でオバマ米大統領（当時）は、中国のサイバー攻撃に非常に深刻な懸念を表明し、あらゆる可能な手段を行使すると経済制裁の適用を示唆したと伝えられている。その一方で、サイバー空間での犯罪の取り締まりに関する米中閣僚級対話の開催に合意した。なお、オーストラリアも、17（平成29）年4月の中国とのハイレベル安全保障対話において、両国が知的財産のサイバー窃取を行わないことに合意している。
35 17（平成29）年11月、米中経済安全保障再検討委員会による年次報告書による。
36 17（平成29）年11月のNATO国防相会合後の記者会見による。
37 16（平成28）年7月に、NATOとEUはサイバーセキュリティを含む、テロ・難民・移民問題などの新たな課題への対処における協力の拡大を目指した共同宣言に署名し、サイバー防衛に関する情報交換を行うなど協力を強化している。
38 13（平成25）年6月、NATO国防相会合では、初めてサイバー防衛を主要課題とし、緊急対応チームを創設するとともに、同年10月までにサイバー防衛体制を安全に稼働させることで合意した。
39 「タリンマニュアル」及び「タリンマニュアル2.0」は、両文書ともに、NATOの公式見解ではなく、あくまでも同プロジェクトに参加したメンバー（米海軍大学のマイケル・シュミット教授がプロジェクトリーダーを務め、欧米などの実務家、国際法学者、サイバー技術専門家などが参加）による独立した成果物と位置づけられている。

4 オーストラリア

オーストラリアは、13（平成25）年1月の「国家安全保障戦略」において、サイバー政策及び作戦の統合が国家安全保障上の最優先課題の一つであるとした。また、16（平成28）年4月、20（平成32）年までの新たな「サイバーセキュリティ戦略」を発表し、国民の安全の確保、民間企業によるサイバーセキュリティへの参画、脅威情報に関する情報共有などについて規定した。

組織面では、政府内のサイバーセキュリティ能力を1カ所に集約した、オーストラリアサイバーセキュリティセンター（ACSC：Australian Cyber Security Center）が、14（平成26）年11月に設置され、政府機関と重要インフラに関する重大なサイバーセキュリティ事案への対処を行っている[40]。ACSCは15（平成27）年7月、初のサイバーセキュリティに関する報告書[41]を出し、オーストラリアに対するサイバー脅威の数、種類、強度がいずれも増加しているとしている。また、17（平成29）年7月、国防省のサイバー戦能力及びシステム強化のため、軍にサイバー部隊を設立した[42]。

5 韓国

韓国では、11（平成23）年8月に「国家サイバーセキュリティ・マスタープラン」が制定され、サイバー攻撃対処における国家情報院[43]の統括機能が明確化されたほか、予防、検知、対応[44]、制度及び基盤の五つの分野を重点的に推進することとされた。国防部門では、国防部にサイバー対策技術チームを創設し、サイバー・ハッキング脅威に対応するとしている[45]。また、「国防サイバー安保戦略書」を作成した上で、「国防サイバー危機対応実務マニュアル」を用意してサイバー危機への迅速な対応手順を定めている。合同参謀本部においては、15（平成27）年にサイバー作戦総括部署を新設し、合同参謀本部議長にサイバー作戦に関する統制権限を付与して、「合同サイバー作戦」教範を発刊するなど、合同参謀本部を中心にサイバー作戦遂行体系を一元化している。

40 ACSCは、豪州犯罪委員会、豪州連邦警察、豪州治安情報機関、豪州通信電子局、豪州コンピュータ緊急対処チーム及び国防情報機構の職員から構成され、サイバー空間における脅威分析や官民双方のインシデント対応を行っている。また、17（平成29）年までに約300名体制になるとしている。
41 同報告書によれば、豪州を狙うサイバー空間の敵には、①外国政府の支援を受けた敵、②重大かつ組織化された犯罪者、③特定の問題に動機づけられた集団や独自の不満を持つ個人がいるとしている。
42 17（平成29）年10月に発表された豪州国際サイバー・エンゲージメント戦略によれば、軍事作戦を支援するための攻撃的なサイバー作戦は、豪州通信電子局及び豪州国防軍が協力して実施することとされている。
43 国家情報院長のもとには、国家のサイバーセキュリティ体制の確立及び改善、関連政策及び機関間の役割調整、大統領の指示事項に関する措置や施策などの重要事項を審議する国家サイバーセキュリティ戦略会議が設置されている。
44 14（平成26）年2月、韓国国防部は、他国を攻撃するサイバー兵器の開発計画を国会で報告したと伝えられている。
45 17（平成29）年4月の韓国・国防日報による。